

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

THIS PAGE BLANK (USPTO)

E P · U S

P C T

特許協力条約

国際調査報告

(法8条、法施行規則第40、41条)
〔PCT18条、PCT規則43、44〕

出願人又は代理人 の書類記号 P 2 4 0 5 6 - P 0	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。	
国際出願番号 PCT/JPO1/00159	国際出願日 (日.月.年) 12.01.01	優先日 (日.月.年) 14.01.00
出願人(氏名又は名称) 松下電器産業株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 4 ページである。 この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
 この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
 この国際出願に含まれる書面による配列表
 この国際出願と共に提出されたフレキシブルディスクによる配列表
 出願後に、この国際調査機関に提出された書面による配列表
 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. 請求の範囲の一部の調査ができない(第I欄参照)。3. 発明の単一性が欠如している(第II欄参照)。4. 発明の名称は 出願人が提出したものと承認する。 次に示すように国際調査機関が作成した。5. 要約は 出願人が提出したものと承認する。 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1ヶ月以内にこの国際調査機関に意見を提出することができる。6. 要約書とともに公表される図は、
第 2 図とする。 出願人が示したとおりである。 なし 出願人は図を示さなかった。 本図は発明の特徴を一層よく表している。

THIS PAGE BLANK (USPTO)

第三欄 要約（第1ページの5の続き）

デジタル情報を記憶する領域を有する記憶媒体と、前記領域からデジタル情報を読み出し、又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記アクセス装置において前記領域を示すアクセス情報を攪乱した攪乱化アクセス情報を用いたチャレンジレスポンス型認証プロトコルにより前記記憶媒体の認証を行うと共に、前記記憶媒体において、前記アクセス装置の認証を行い、共に正当性が認証された場合には、前記アクセス装置によって前記攪乱化アクセス情報から分離されたアクセス情報に応じた前記記憶媒体の前記領域にデジタル情報を読み出し、又は前記領域に書き込む。

THIS PAGE BLANK (USPTO)

(12)特許協力条約に基づいて公開された国際出願

(19)世界知的所有権機関
国際事務局



(43)国際公開日
2001年7月19日 (19.07.2001)

PCT

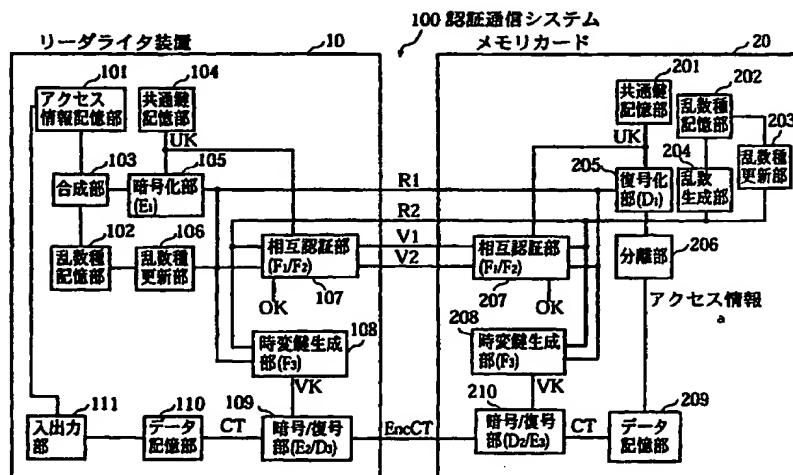
(10)国際公開番号
WO 01/52474 A1

(51) 国際特許分類:	H04L 9/32, 9/08, G06F 17/60	(71) 出願人(米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006番地 Osaka (JP).
(21) 国際出願番号:	PCT/JP01/00159	
(22) 国際出願日:	2001年1月12日 (12.01.2001)	
(25) 国際出願の言語:	日本語	
(26) 国際公開の言語:	日本語	
(30) 優先権データ:		
特願2000-006989	2000年1月14日 (14.01.2000)	JP
特願2000-041317	2000年2月18日 (18.02.2000)	JP
		(72) 発明者; および
		(75) 発明者/出願人(米国についてのみ): 柴田 修 (SHIBATA, Osamu) [JP/JP]; 〒570-0032 大阪府守口市菊水通1-16-22 Osaka (JP). 湯川泰平 (YUGAWA, Taihei) [JP/JP]; 〒631-0041 奈良県奈良市学園大和町6-708-1-513 Nara (JP). 関部 勉 (SEKIBE, Tsutomu) [JP/JP]; 〒573-0047 大阪府枚方市山之上5-49-34 Osaka (JP). 廣田照人 (HIROTA, Teruto) [JP/JP]; 〒570-0015 大阪府守口市梶町1-20-1-306 Osaka (JP). 斎藤義行 (SAITO, Yoshiyuki) [JP/JP]; 〒576-0053 大阪府交野市郡津1-1-611 Osaka (JP). 大竹俊彦 (OTAKE, Toshihiko)

[統葉有]

(54) Title: AUTHENTICATION COMMUNICATION DEVICE AND AUTHENTICATION COMMUNICATION SYSTEM

(54)発明の名称: 認証通信装置及び認証通信システム



10...READER/WRITER
101...ACCESS INFORMATION STORAGE SECTION
104...COMMON KEY STORAGE SECTION
103...SYNTHEZISING SECTION
105...ENCRYPTING SECTION
102...RANDOM NUMBER TYPE STORAGE SECTION
106...RANDOM NUMBER TYPE UPDATING SECTION
107...MUTUAL AUTHENTICATING SECTION
108...TIME-VARYING KEY GENERATING SECTION
111...I/O SECTION
110...DATA STORAGE SECTION
109...ENCRYPTING/DECRYPTING SECTION
100...AUTHENTICATION COMMUNICATION SYSTEM
20...MEMORY CARD

201...COMMON KEY STORAGE SECTION
202...RANDOM NUMBER TYPE STORAGE SECTION
203...RANDOM NUMBER TYPE UPDATING SECTION
205...DECRYPTING SECTION
204...RANDOM NUMBER GENERATING SECTION
207...MUTUAL AUTHENTICATING SECTION
206...SEPARATING SECTION
208...TIME-VARYING KEY GENERATING SECTION
210...ENCRYPTING/DECRYPTING SECTION
209...DATA STORAGE SECTION
a...ACCESS INFORMATION

(57) Abstract: An authentication communication device comprises a storage medium having an area for storing digital information therein and an access unit for reading digital information from the area and writing digital information in the area. The access unit authenticates the storage medium according to a challenge response authentication protocol using disturbed access information produced by disturbing access information indicative of the area. The access unit is authenticated by the storage medium. When the validity is of both the storage medium and the access unit authenticated, the access unit reads out digital information from the area of the storage medium corresponding to access information separated from the disturbed access information or writes digital information therein.

WO 01/52474 A1

[統葉有]



[JP/JP]; 〒662-0095 兵庫県西宮市美作町5-12 Hyogo (JP). (84) 指定国(広域): ヨーロッパ特許(DE, FR, GB, NL).

(74) 代理人: 中島司朗(NAKAJIMA, Shiro); 〒531-0072 大阪府大阪市北区豊崎三丁目2番1号 淀川5番館6F Osaka (JP).

(81) 指定国(国内): AU, CN, ID, KR, MX, US.

添付公開書類:
— 國際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

デジタル情報を記憶する領域を有する記憶媒体と、前記領域からデジタル情報を読み出し、又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記アクセス装置において前記領域を示すアクセス情報を攪乱した攪乱化アクセス情報を用いたチャレンジレスポンス型認証プロトコルにより前記記憶媒体の認証を行うと共に、前記記憶媒体において、前記アクセス装置の認証を行い、共に正当性が認証された場合には、前記アクセス装置によって前記攪乱化アクセス情報から分離されたアクセス情報に応じた前記記憶媒体の前記領域にデジタル情報を読み出し、又は前記領域に書き込む。

明細書

認証通信装置及び認証通信システム

5 技術分野

本発明は、デジタル著作物を機器と記録媒体との間で転送する場合において、機器と記録媒体との間で、相互に正当性を認証する技術に関する。

10 背景技術

近年、デジタル情報圧縮技術の進展と、インターネットに代表されるグローバルな通信インフラの爆発的な普及によって、音楽、画像、映像、ゲームなどの著作物をデジタル著作物として通信回線を介して各家庭に配信することが実現されている。

15 デジタル著作物の著作権者の権利や、流通業者の利益を保護するための流通配信システムを確立するために、通信の傍受、盗聴、なりすましなどによる著作物の不正な入手や、受信したデータを記録している記録媒体からの違法な複製、違法な改竄などの不正行為を防止することが課題となっており、正規のシステムかどうかの判別を行ったり、データスクランブルを行う暗号及び認証などの著作物保護技術が必要とされている。

20 著作物保護技術については、従来より様々なものが知られており、代表的なものとして、著作物の保護を要する機密データが格納されている機密データ記憶領域にアクセスする際に、機器間で乱数と応答値の交換を行って、相互に正当性を認証しあい、正当である場合のみ、アクセスを許可するチャレンジレスポンス型の相互認証技術がある。

25 しかしながら、例えば、相互認証を正規な機器を用いて行った後に、正当機器になりすまして、機密データ記憶領域にアクセスすることによ

り、機密データを不正に入手する行為が考えられる。

発明の開示

そこで本発明はかかる問題点に鑑みてなされたものであり、機密データ記憶領域にアクセスするための情報が漏洩されないアクセス装置、記録媒体、認証通信システム、認証通信方法及び認証通信プログラムを記録している記録媒体を提供することを目的とする。

上記目的を達成するために本発明は、デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証フェーズと、前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証フェーズと、前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズとを含むことを特徴とする。

これによって、相互認証と同時に、機密のデータを記録している機密データ記憶領域にアクセスするための情報を攪乱して転送するので、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。

また、仮に、機密データ記憶領域にアクセスするための情報が、不正なりすましにより、別の情報に改竄されて転送された場合であっても、相互認証が成功しないので、機密データ記憶領域にアクセスできないようにすることができる。

図面の簡単な説明

図1は、認証通信システム100の具体的な構成例としての認証通信システム30及び31の外観を示す。図1(a)は、パソコン用コンピュータとメモリカード20から構成される認証通信システム30の外観を示し、図1(b)は、ヘッドホンステレオ、メモリカード20及びヘッドホンから構成される認証通信システム31の外観を示す。

図2は、認証通信システム100を構成するリーダライタ装置10及びメモリカード20のそれぞれ構成を示すブロック図である。

図3は、アクセス情報、乱数種及び乱数化アクセス情報のデータ構造を示す。図4は、認証通信システム100の動作を示すフローチャートであり、特に、メモリカードに記憶されている情報を読み出す場合を想定したものである。図5に続く。

図5は、認証通信システム100の動作を示すフローチャートである。

図4から続く。

図6は、認証通信システム100の動作を示すフローチャートであり、特に、リーダライタ装置10は、メモリカードに情報を書き込む装置であると想定した場合のものである。

図7は、別の実施の形態としての、認証通信システム100aの構成を示すブロック図である。

図8は、認証通信システム100aに固有の動作を示すフローチャートである。

図9は、別の実施の形態としての、認証通信システム100bの構成を示すブロック図である。

図10は、認証通信システム100bに固有の動作を示すフローチャートである。

発明を実施するための最良の形態

本発明に係る一つの実施の形態としての認証通信システム100について説明する。

1. 認証通信システム 100 の外観と利用形態

認証通信システム 100 の具体的な構成例としての認証通信システム 30 及び 31 の外観図を図 1 (a) 及び (b) に示す。

図 1 (a) に示すように、認証通信システム 30 は、パーソナルコンピュータとメモリカード 20 から構成される。パーソナルコンピュータは、ディスプレイ部、キーボード、スピーカ、マイクロプロセッサ、RAM、ROM、ハードディスクユニットなどを備えており、通信回線を経由してインターネットに代表されるネットワークに接続されている。メモリカード 20 は、メモリカード挿入口から挿入され、パーソナルコンピュータに装着される。

図 1 (b) に示すように、認証通信システム 31 は、ヘッドホンステレオ、メモリカード 20 及びヘッドホンから構成される。メモリカード 20 は、ヘッドホンステレオのメモリカード挿入口から挿入されて、ヘッドホンステレオに装着される。ヘッドホンステレオは、上面に複数の操作ボタンが配置されており、別の側面にヘッドホンが接続されている。

利用者は、メモリカード 20 をパーソナルコンピュータに装着し、インターネットを経由して、外部の Web サーバ装置から音楽などのデジタル著作物を取り込み、取り込んだデジタル著作物をメモリカード 20 に書き込む。次に、利用者は、デジタル著作物の記録されているメモリカード 20 をヘッドホンステレオに装着し、メモリカード 20 に記録されているデジタル著作物をヘッドホンステレオにより再生して、楽しむ。

ここで、パーソナルコンピュータとメモリカード 20との間において、また、ヘッドホンステレオとメモリカード 20との間において、チャレンジレスポンス型の認証プロトコルによる各機器の正当性の認証を行い、相互に正当な機器であることが認証された場合にのみ、各機器間でデジタル著作物の転送が行われる。

2. 認証通信システム 100 の構成

認証通信システム 100 は、図 2 に示すように、リーダライタ装置 1

0 及びメモリカード 20 から構成される。ここで、リーダライタ装置 10 は、図 1 (a) 及び (b) に示すパーソナルコンピュータ及びヘッドホンステレオに相当する。

2. 1 リーダライタ装置 10 の構成

5 リーダライタ装置 10 は、アクセス情報記憶部 101、乱数種記憶部 102、合成部 103、共通鍵記憶部 104、暗号化部 105、乱数種更新部 106、相互認証部 107、時変鍵生成部 108、暗号復号部 109、データ記憶部 110 及び入出力部 111 から構成されている。

10 リーダライタ装置 10 は、具体的には、マイクロプロセッサ、RAM、ROM その他を備え、ROM などにコンピュータプログラムが記録されており、マイクロプロセッサは、前記コンピュータプログラムに従って動作する。

(1) 入出力部 111

15 入出力部 111 は、利用者の操作を受け付けて、メモリカード 20 のデータ記憶部 209 に記憶されている音楽情報にアクセスするためのアクセス情報を生成する。アクセス情報は、図 3 に示すように、32 ビット長であり、メモリカード 20 のデータ記憶部の領域のアドレスを示すアドレス情報と、前記領域のサイズを示すサイズ情報とから構成される。アドレス情報は、24 ビット長であり、サイズ情報は、8 ビット長である。

20 また、入出力部 111 は、データ記憶部 110 から音楽情報 CT を読み出し、読み出した音楽情報 CT を音声信号に変換して出力する。

25 また、入出力部 111 は、利用者の操作を受け付けて、外部から音楽情報 CT を取得し、取得した音楽情報 CT をデータ記憶部 110 へ書き込む。

(2) アクセス情報記憶部 101

アクセス情報記憶部 101 は、具体的には、半導体メモリから構成され、アクセス情報を記憶する領域を備えている。

(3) 亂数種記憶部 102

乱数種記憶部 102 は、具体的には、半導体メモリから構成され、図 3 に示すような 64 ビット長の乱数種をあらかじめ記憶している。乱数種は、装置の製造時に記録される。

5 乱数種記憶部 102 は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

(4) 合成部 103

合成部 103 は、アクセス情報記憶部 101 からアクセス情報を読み出し、乱数種記憶部 102 から乱数種を読み出す。次に、図 3 に示すように、読み出した前記アクセス情報と、読み出した前記乱数種の下位 3 10 2 ビットとを結合して、64 ビット長の乱数化アクセス情報を生成する。生成した乱数化アクセス情報を暗号化部 105 へ出力する。

(5) 共通鍵記憶部 104

共通鍵記憶部 104 は、具体的には、半導体メモリから構成され、5 15 6 ビット長の共通鍵 UK を記憶する領域を備えている。リーダライタ装置 10 は、メモリカード 20 から共通鍵記憶部 201 に記憶されている共通鍵 UK を秘密に取得し、共通鍵記憶部 104 は、取得した共通鍵 UK を記憶する。

共通鍵記憶部 104 は、外部から直接アクセスできる手段を有してお 20 らず、プロテクトされている記憶手段である。

(6) 暗号化部 105

暗号化部 105 は、共通鍵記憶部 104 から共通鍵 UK を読み出し、合成部 103 から乱数化アクセス情報を受け取る。次に、暗号化部 10 25 5 は、共通鍵 UK を用いて、受け取った乱数化アクセス情報を暗号アルゴリズム E 1 を施して暗号化アクセス情報 R 1 を生成する。ここで、暗号化部 105 は、暗号アルゴリズム E 1 として、DES (Data Encryption Standard) を用いる。

次に、暗号化部 105 は、生成した暗号化アクセス情報 R 1 を、相互

認証部 107 と、乱数種更新部 106 と、時変鍵生成部 108 とへ出力する。また、生成した暗号化アクセス情報 R1 を、メモリカード 20 の復号化部 205 と、相互認証部 207 と、時変鍵生成部 208 とへ出力する。

5 このようにして生成された暗号化アクセス情報 R1 は、アクセス情報に攪乱 (scramble) 処理を施して得られる攪乱化情報である。

(7) 亂数種更新部 106

乱数種更新部 106 は、暗号化部 105 から暗号化アクセス情報 R1 を受け取り、受け取った暗号化アクセス情報 R1 を新たな乱数種として
10 亂数種記憶部 102 へ上書きする。

(8) 相互認証部 107

相互認証部 107 は、暗号化アクセス情報 R1 を受け取り、共通鍵記憶部 104 から共通鍵 UK を読み出し、受け取った R1 と共に UK を用いて、式 1 により、応答値 V2' を算出する。

15 (式 1) $V2' = F1(R1, UK) = SHA(R1 + UK)$

ここで、関数 F1 (a, b) は、一例として、a と b とを結合し、その結合結果に対して SHA (Secure Hash Algorithm) を施す関数である。なお、+ は、結合を示す演算子である。

相互認証部 107 は、相互認証部 207 から応答値 V2 を受け取る。

20 次に、相互認証部 107 は、V2 と V2' とが一致するか否かを判断し、一致しない場合には、メモリカード 20 が不正な装置であると認定し、他の構成部に対して以降の動作の実行を禁止する。一致する場合は、相互認証部 107 は、メモリカード 20 が正当な装置であると認定し、他の構成部に対して以降の動作の実行を許可する。

25 また、相互認証部 107 は、乱数生成部 204 から乱数 R2 を受け取り、受け取った乱数 R2 と、前記共通鍵 UK とを用いて、式 2 により、応答値 V1 を算出し、算出した応答値 V1 を相互認証部 207 へ出力する。

(式2) $V_1 = F_2(R_2, UK) = SHA(R_2 + UK)$

(9) 時変鍵生成部108

時変鍵生成部108は、メモリカード20が正当な装置であると認定され、動作の実行を許可される場合に、暗号化アクセス情報R1と乱数R2とを受け取り、R1とR2とから、式3を用いて時変鍵VKを生成する

(式3) $VK = F_3(R_1, R_2) = SHA(R_1 + R_2)$

次に、時変鍵生成部108は、生成した時変鍵VKを暗号復号部109へ出力する。

(10) 暗号復号部109

暗号復号部109は、時変鍵生成部108から時変鍵VKを受け取る。

暗号復号部109は、暗号復号部210から暗号化音楽情報E n c C Tを受け取り、前記時変鍵VKを用いて、暗号化音楽情報E n c C Tに復号アルゴリズムD3を施して音楽情報CTを生成し、生成した音楽情報CTをデータ記憶部110へ書き込む。

ここで、暗号復号部109は、復号アルゴリズムE3として、DESを用いる。

また、暗号復号部109は、データ記憶部110から音楽情報CTを読み出し、前記時変鍵VKを用いて、音楽情報CTに暗号アルゴリズムE2を施して暗号化音楽情報E n c C Tを生成し、生成した暗号化音楽情報E n c C Tを暗号復号部210へ出力する。

ここで、暗号復号部109は、暗号アルゴリズムE2として、DESを用いる。

(11) データ記憶部110

データ記憶部110は、具体的には、半導体メモリから構成され、音楽情報CTを記憶する領域を備えている。

2. 2 メモリカード20

メモリカード20は、共通鍵記憶部201、乱数種記憶部202、乱

数種更新部203、乱数生成部204、復号化部205、分離部206、相互認証部207、時変鍵生成部208、データ記憶部209及び暗号復号部210から構成されている。

(1) 共通鍵記憶部201

5 共通鍵記憶部201は、具体的には、半導体メモリから構成され、6ビット長の共通鍵UKを記憶している。共通鍵UKは、メモリカード20の製造時に記録される。

10 共通鍵記憶部201は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

15 (2) 亂数種記憶部202

乱数種記憶部202は、具体的には、半導体メモリから構成され、64ビット長の乱数種をあらかじめ記憶している。乱数種は、メモリカード20の製造時に記録される。

15 亂数種記憶部202は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

(3) 亂数生成部204

乱数生成部204は、乱数種記憶部202から乱数種を読み出し、読み出した乱数種を用いて64ビット長の乱数R2を生成し、生成した乱数R2を乱数種更新部203と、相互認証部207と、時変鍵生成部208とへ出力し、生成した乱数R2をリーダライタ装置10の相互認証部107と、時変鍵生成部108とへ出力する。

(4) 亂数種更新部203

乱数種更新部203は、乱数生成部204から乱数R2を受け取り、受け取った乱数R2を新たな乱数種として乱数種記憶部202へ上書きする。

(5) 復号化部205

復号化部205は、共通鍵記憶部201から共通鍵UKを読み出し、暗号化部105から暗号化アクセス情報R1を受け取る。次に、読み出

した共通鍵UKを用いて、受け取った暗号化アクセス情報R1に、復号アルゴリズムD1を施して、乱数化アクセス情報を生成し、生成した乱数化アクセス情報を分離部206へ出力する。

ここで、復号化部205は、復号アルゴリズムD1として、DESを用いる。復号アルゴリズムD1は、暗号アルゴリズムE1により生成された暗号文を復号する。

(6) 分離部206

分離部206は、復号化部205から乱数化アクセス情報を受け取り、受け取った乱数化アクセス情報から、その上位32ビットのデータをアクセス情報として分離し、アクセス情報をデータ記憶部209へ出力する。

(7) 相互認証部207

相互認証部207は、共通鍵記憶部201から共通鍵UKを読み出し、暗号化アクセス情報R1を受け取り、受け取ったR1と共通鍵UKとを用いて、式4により、応答値V2を算出し、算出したV2をリーダライタ装置10の相互認証部107へ出力する。

$$(式4) V2 = F1(R1, UK) = SHA(R1 + UK)$$

ここで、F1は、式1に示すF1と同じ関数であればよい。

また、相互認証部207は、乱数生成部204から乱数R2を受け取り、受け取った乱数R2と、前記共通鍵UKとを用いて、式5により、応答値V1'を算出する。

$$(式5) V1' = F2(R2, UK) = SHA(R2 + UK)$$

ここで、F2は、式2に示すF2と同じ関数であればよい。

次に、相互認証部207は、相互認証部107からV1を受け取り、V1とV1'が一致するか否かを判断し、一致しない場合には、リーダライタ装置10が不正な装置であると認定し、他の構成部に対して以下の動作の実行を禁止する。一致する場合には、相互認証部207は、リーダライタ装置10が正当な装置であると認定し、他の構成部に対し

て以降の動作の実行を許可する。

(8) 時変鍵生成部 208

時変鍵生成部 208 は、リーダライタ装置 10 が正当な装置であると認定され、動作の実行を許可される場合に、暗号化アクセス情報 R1 と乱数 R2 とを受け取り、R1 と R2 とから、式 6 を用いて時変鍵 VK を生成する

$$(式 6) \quad VK = F_3(R_1, R_2) = SHA(R_1 + R_2)$$

ここで、F3 は、式 3 に示す関数 F3 と同じである。

次に、時変鍵生成部 208 は、生成した時変鍵 VK を暗号復号部 210 へ出力する。

(9) データ記憶部 209

データ記憶部 209 は、具体的には、半導体メモリから構成され、音楽情報 CT を記憶する領域を備えている。

(10) 暗号復号部 210

暗号復号部 210 は、時変鍵生成部 208 から時変鍵 VK を受け取る。

暗号復号部 210 は、暗号復号部 109 から暗号化音楽情報 EncCT を受け取り、前記時変鍵 VK を用いて、暗号化音楽情報 EncCT に復号アルゴリズム D2 を施して音楽情報 CT を生成し、生成した音楽情報 CT をデータ記憶部 209 の前記アクセス情報により示される領域へ書き込む。

ここで、暗号復号部 210 は、復号アルゴリズム D2 として、DES を用いる。復号アルゴリズム D2 は、暗号アルゴリズム E2 により生成された暗号文を復号する。

また、暗号復号部 210 は、データ記憶部 209 の前記アクセス情報により示される領域から音楽情報 CT を読み出し、前記時変鍵 VK を用いて、音楽情報 CT に暗号アルゴリズム E3 を施して暗号化音楽情報 EncCT を生成し、生成した暗号化音楽情報 EncCT を暗号復号部 109 へ出力する。

ここで、暗号復号部210は、暗号アルゴリズムE3として、DESを用いる。復号アルゴリズムD3は、暗号アルゴリズムE3により生成された暗号文を復号する。

3. 認証通信システム100の動作

5 (1) 読み出し動作

認証通信システム100を構成するリーダライタ装置10及びメモリカード20の動作について、図4～図5に示すフローチャートを用いて説明する。

なお、ここでは、リーダライタ装置10は、図1(b)に示すヘッドホンステレオのように、メモリカードに記憶されている情報を読み出す装置であると想定して説明する。

合成部103は、乱数種記憶部102から乱数種を読み出し、アクセス情報記憶部101からアクセス情報を読み出し、読み出した前記乱数種と読み出した前記アクセス情報を合成して、乱数化アクセス情報を生成し(ステップS101)、暗号化部は、共通鍵記憶部104から共通鍵を読み出し、読み出した前記共通鍵を用いて乱数化アクセス情報を暗号化して暗号化アクセス情報R1を生成し(ステップS102)、相互認証部107は、 $V2' = F1(R1)$ を算出し(ステップS103)、乱数種更新部106は、生成された乱数化アクセス情報を新たな乱数種として乱数種記憶部102に上書きする(ステップS104)。

暗号化部105は、生成した暗号化アクセス情報R1をメモリカード20へ出力し、メモリカードの相互認証部207は、暗号化アクセス情報R1を受け取る(ステップS105)。

相互認証部207は、 $V2 = F1(R1)$ を算出し(ステップS106)、 $V2$ をリーダライタ装置10の相互認証部107へ出力し、相互認証部107は、 $V2$ を受け取る(ステップS107)。

相互認証部107は、 $V2$ と $V2'$ とが一致するか否かを判断し、一致しない場合には(ステップS108)、メモリカード20が不正な装置

であると認定し、以後の動作を中止する。

一致する場合には（ステップS108）、相互認証部107は、メモリカード20が正当な装置であると認定し、メモリカード20の乱数生成部204は、乱数種記憶部202から乱数種を読み出し、読み出した乱数種を用いて乱数R2を生成し（ステップS109）、相互認証部207は、 $V_1' = F_2(R_2)$ を算出し（ステップS110）、乱数種更新部203は、生成された乱数R2を新たに乱数種として乱数種記憶部202に上書きする（ステップS111）。次に、乱数生成部204は、生成した乱数R2をリーダライタ装置10の相互認証部107へ出力し、相互認証部107は、乱数R2を受け取り（ステップS112）、相互認証部107は、 $V_1 = F_2(R_2)$ を生成し（ステップS113）、生成した V_1 をメモリカード20の相互認証部207へ出力し、相互認証部207は、 V_1 を受け取る（ステップS114）。

次に、相互認証部207

相互認証部207は、 V_1 と V_1' とが一致するか否かを判断し、一致しない場合には（ステップS115）、リーダライタ装置10が不正な装置であると認定し、以後の動作を中止する。

一致する場合には（ステップS115）、相互認証部207は、リーダライタ装置10が正当な装置であると認定し、リーダライタ装置10の時変鍵生成部108は、R1とR2とを用いて時変鍵VKを生成する（ステップS121）。メモリカード20の復号化部205は、共通鍵記憶部201から共通鍵UKを読み出し、読み出した共通鍵UKを用いてR1を復号して乱数化アクセス情報を生成し（ステップS122）、分離部206は、乱数化アクセス情報を分離し（ステップS123）、時変鍵生成部208は、R1とR2とを用いて時変鍵VKを生成し（ステップS124）、暗号復号部210は、アクセス情報により示されるデータ記憶部209の領域から音楽情報CTを読み出し（ステップS125）、暗号復号部210は、生成された時変鍵VKを用いて読み出

した前記音楽情報CTを暗号化して暗号化音楽情報EnccCTを生成し(ステップS126)、生成した暗号化音楽情報EnccCTをリーダライタ装置10の暗号復号部109へ出力する(ステップS127)。

5 暗号復号部109は、時変鍵VKを用いて暗号化音楽情報EnccCTを復号して音楽情報CTを生成してデータ記憶部110へ書き込み(ステップS128)、入出力部111は、音楽情報CTをデータ記憶部110から読み出し、読み出した音楽情報CTを音声信号に変換して出力する(ステップS129)。

(2) 書き込み動作

10 認証通信システム100を構成するリーダライタ装置10及びメモリカード20の動作について、図6に示すフローチャートを用いて説明する。

15 ここでは、リーダライタ装置10は、図1(a)に示すパーソナルコンピュータのように、メモリカードに情報を書き込む装置であると想定して説明する。また、読み出し動作と書き込み動作は類似しているので、相違点のみについて説明する。

図4～図5のフローチャートのステップS125～S129を、図6に示すステップに置き換えると認証通信システム100の書き込み動作となる。

20 暗号復号部109は、データ記憶部110から音楽情報CTを読み出し(ステップS131)、時変鍵VKを用いて読み出した音楽情報CTを暗号化して暗号化音楽情報CTを生成し(ステップS132)、生成した暗号化音楽情報CTをメモリカード20の暗号復号部210へ出力し、暗号復号部210は、暗号化音楽情報CTを受け取る(ステップS133)。

25 暗号復号部210は、暗号化音楽情報EnccCTを時変鍵VKを用いて復号して音楽情報CTを生成し(ステップS134)、生成した音楽情報CTを前記アクセス情報で示されるデータ記憶部209内の領域に書

き込む（ステップS135）。

4.まとめ

以上説明したように、相互認証と同時に、機密のデータを記録している機密データ記憶領域にアクセスするための情報を攪乱して転送するの
5 で、機密データ記憶領域にアクセスするための情報の機密性を高めること
ができる。

また、仮に機密データ記憶領域にアクセスするための情報が、不正な
なりすましにより、別の情報に改竄されて転送された場合であっても、
相互認証が確立しないので、機密データ記憶領域にアクセスできないよ
うにすることができる。
10

また、乱数の更新に機密データ記憶領域にアクセスするためのアクセス
情報が関連していないので、乱数の周期性を高めることができる。

5.認証通信システム100a

認証通信システム100の変形例としての認証通信システム100a

15 について説明する。

5.1 認証通信システム100aの構成

認証通信システム100aは、図7に示すように、リーダライタ装置
10aとメモリカード20とから構成される。

メモリカード20は、図2に示すメモリカード20と同じであるので、
20 ここでは、説明を省略する。

リーダライタ装置10aは、アクセス情報記憶部101、乱数種記憶
部102、合成部103、共通鍵記憶部104、暗号化部105、乱数
種更新部106、相互認証部107、時変鍵生成部108、暗号復号部
109、データ記憶部110、入出力部111及び乱数生成部112か
ら構成されている。
25

リーダライタ装置10との相違点を中心として、以下に説明する。その他の点については、リーダライタ装置10と同じであるので、説明を省略する。

5 (1) 亂数生成部 112

乱数生成部 112 は、乱数種記憶部 102 から乱数種を読み出し、読み出した乱数種を用いて 64 ビット長の乱数を生成し、生成した乱数を合成部 103 と乱数種更新部 106 とへ出力する。

5 (2) 亂数種更新部 106

乱数種更新部 106 は、乱数生成部 112 から乱数を受け取り、受け取った乱数を新たな乱数種として乱数種記憶部 102 へ上書きする。

(3) 合成部 103

合成部 103 は、乱数生成部 112 から乱数を受け取り、アクセス情報記憶部 101 からアクセス情報を読み出し、受け取った前記乱数と読み出した前記アクセス情報を合成して、乱数化アクセス情報を生成する。

5. 2 認証通信システム 100a の動作

認証通信システム 100a の動作について、図 8 に示すフローチャートを用いて説明する。

乱数生成部 112 は、乱数種記憶部 102 から乱数種を読み出し（ステップ S201）、読み出した乱数種を用いて 64 ビット長の乱数を生成し（ステップ S202）、乱数種更新部 106 は、乱数生成部 112 から乱数を受け取り、受け取った乱数を新たな乱数種として乱数種記憶部 102 へ上書きする（ステップ S203）。次に、合成部 103 は、乱数生成部 112 から乱数を受け取り、アクセス情報記憶部 101 からアクセス情報を読み出し、受け取った前記乱数と読み出した前記アクセス情報を合成して、乱数化アクセス情報を生成する（ステップ S204）。

次に、図 4 のステップ S102 へ続く。以下は、認証通信システム 100 の動作と同じであるので、説明を省略する。

5. 3 まとめ

以上説明したように、乱数の更新に機密データ記憶領域にアクセスするためのアクセス情報が関連していないので、乱数の周期性を高めるこ

とができる。

6. 認証通信システム 100 b

認証通信システム 100 a の変形例としての認証通信システム 100 b について説明する。

5 6. 1 認証通信システム 100 b の構成

認証通信システム 100 b は、図 9 に示すように、リーダライタ装置 10 b とメモリカード 20 b とから構成される。

(1) リーダライタ装置 10 b の構成

リーダライタ装置 10 b は、アクセス情報記憶部 101、乱数種記憶部 102、合成部 103、共通鍵記憶部 104、暗号化部 105、乱数種更新部 106、相互認証部 107、時変鍵生成部 108、データ記憶部 110、入出力部 111、乱数生成部 112、コンテンツ鍵生成部 113、暗号化部 114、コンテンツ付加情報記憶部 115、暗号復号部 116 及び暗号化部 117 から構成されている。

15 以下において、リーダライタ装置 10 a との相違点を中心として説明する。その他の点については、リーダライタ装置 10 a と同じであるので、説明を省略している。

(a) 入出力部 111

20 入出力部 111 は、利用者の操作によりコンテンツ付加情報の入力を受け付け、受け付けたコンテンツ付加情報をコンテンツ付加情報記憶部 115 に書き込む。

ここで、コンテンツ付加情報の一例は、コンテンツの再生回数、使用期間であり、コンテンツ付加情報は、8 ビット長である。

25 また、入出力部 111 は、利用者の操作によりコンテンツデータ CD を取得し、取得したコンテンツデータ CD をデータ記憶部 110 に書き込む。

ここで、コンテンツデータ CD は、一例として音楽コンテンツ情報である。

(b) 亂数生成部 112

乱数生成部 112 は、生成した乱数 R3 をコンテンツ鍵生成部 113 へ出力する。

(c) コンテンツ鍵生成部 113

5 コンテンツ鍵生成部 113 は、コンテンツ付加情報記憶部 115 からコンテンツ付加情報を読み出し、乱数生成部 112 から乱数 R3 を受け取り、乱数 R3 と読み出したコンテンツ付加情報を用いて、式 7 により、コンテンツ鍵 CK を生成する。ここで、コンテンツ鍵 CK は、64 ビット長である。

10 (式 7) $CK = F_4(R3, \text{コンテンツ付加情報})$

$$= \text{コンテンツ付加情報 (8 ビット長)} + R3 \text{ の下位 } 56 \text{ ビット}$$

ここで、+ は、データとデータの結合を示す演算子である。

次に、コンテンツ鍵生成部 113 は、生成したコンテンツ鍵 CK を暗号化部 114 と、暗号化部 117 とへ出力する。

(d) 暗号化部 114

暗号化部 114 は、コンテンツ鍵生成部 113 からコンテンツ鍵 CK を受け取り、共通鍵記憶部 104 から共通鍵 UK を読み出し、読み出した共通鍵 UK を用いて、受け取ったコンテンツ鍵 CK に暗号化アルゴリズム E4 を施して暗号化コンテンツ鍵 Enc CK を生成し、生成した暗号化コンテンツ鍵 Enc CK を暗号復号部 116 へ出力する。

ここで、暗号化部 114 は、暗号アルゴリズム E4 として、DES を用いる。(e) 暗号復号部 116

暗号復号部 116 は、暗号化部 114 から暗号化コンテンツ鍵 Enc CK を受け取り、受け取った暗号化コンテンツ鍵 Enc CK に、時変鍵 VK を用いて、暗号アルゴリズム E2 を施して Enc (Enc CK) を生成し、生成した Enc (Enc CK) を暗号復号部 211 へ出力する。

ここで、暗号復号部 116 は、暗号アルゴリズム E2 として、DES

を用いる。

(f) 暗号化部 117

暗号化部 117 は、データ記憶部 110 からコンテンツデータ CD を読み出し、読み出したコンテンツデータ CD に、コンテンツ鍵 CK を用いて、暗号化アルゴリズム E5 を施して暗号化コンテンツデータ Enc CD を生成する。次に、暗号化部 117 は、生成した暗号化コンテンツデータ Enc CD をデータ記憶部 213 へ出力する。

ここで、暗号化部 117 は、暗号アルゴリズム E5 として、DES を用いる。

(2) メモリカード 20b の構成

メモリカード 20b は、共通鍵記憶部 201、乱数種記憶部 202、乱数種更新部 203、乱数生成部 204、復号化部 205、分離部 206、相互認証部 207、時変鍵生成部 208、暗号復号部 211、鍵データ記憶部 212 及びデータ記憶部 213 から構成されている。

以下において、メモリカード 20 との相違点を中心として説明する。その他の点については、メモリカード 20 と同じであるので、説明を省略している。

(a) 時変鍵生成部 208

時変鍵生成部 208 は、時変鍵 VK を暗号復号部 211 へ出力する。

(b) 暗号復号部 211

暗号復号部 211 は、時変鍵生成部 208 から時変鍵 VK を受け取り、暗号復号部 116 から Enc (Enc CK) を受け取る。

次に、暗号復号部 211 は、時変鍵 VK を用いて Enc (Enc CK) に復号アルゴリズム D2 を施して暗号化コンテンツ鍵 Enc CK を生成し、生成した暗号化コンテンツ鍵 Enc CK を前記アクセス情報により示される鍵データ記憶部 212 の領域に書き込む。

(c) 鍵データ記憶部 212

鍵データ記憶部 212 は、暗号化コンテンツ鍵 Enc CK を記憶する

領域を備える。

(d) データ記憶部 213

データ記憶部 213 は、暗号化コンテンツデータ Enc CD を受け取り、受け取った暗号化コンテンツデータ Enc CD を記憶する。

5 6. 2 認証通信システム 100b の動作

認証通信システム 100b の動作は、認証通信システム 100a の動作に類似している。ここでは、認証通信システム 100a との相違点についてのみ説明する。

10 認証通信システム 100b の動作は、認証通信システム 100a の動作を示すフローチャートのうち、ステップ S121 以降を図 10 に示すフローチャートに置き換えたフローチャートにより示される。

15 コンテンツ鍵生成部 113 は、コンテンツ付加情報記憶部 115 からコンテンツ付加情報を読み出し（ステップ S301）、乱数生成部 112 は、生成した乱数 R3 をコンテンツ鍵生成部 113 へ出力し、コンテンツ鍵生成部 113 は、乱数生成部 112 から R3 を受け取り、R3 と読み出したコンテンツ付加情報を用いて、コンテンツ鍵 CK を生成し、生成したコンテンツ鍵 CK を暗号化部 114 と、暗号化部 117 とへ出力し（ステップ S302）、暗号化部 114 は、コンテンツ鍵生成部 113 からコンテンツ鍵 CK を受け取り、共通鍵記憶部 104 から共通鍵 UK 20 を読み出し、読み出した共通鍵 UK を用いて、受け取ったコンテンツ鍵 CK に暗号化アルゴリズム E4 を施して暗号化コンテンツ鍵 Enc CK を生成し、生成した暗号化コンテンツ鍵 Enc CK を暗号復号部 116 へ出力する（ステップ S303）。次に、暗号復号部 116 は、暗号化コンテンツ鍵 Enc CK を受け取り、受け取った暗号化コンテンツ鍵 Enc 25 CK に時変鍵 VK を用いて暗号アルゴリズム E2 を施して Enc (Enc CK) を生成し（ステップ S304）、暗号復号部 116 は、生成した Enc (Enc CK) を暗号復号部 211 へ出力し、暗号復号部 211 は、Enc (Enc CK) を受け取り（ステップ S305）、暗号復号

部211は、E n c (E n c C K) に時変鍵VKを用いて復号アルゴリズムD2を施して暗号化コンテンツ鍵E n c C Kを生成し、生成した暗号化コンテンツ鍵E n c C Kを前記アクセス情報により示される鍵データ記憶部212の領域に書き込む(ステップS306)。

5 暗号化部117は、データ記憶部110からコンテンツデータCDを読み出し(ステップS307)、読み出したコンテンツデータCDにコンテンツ鍵CKを用いて暗号化アルゴリズムE5を施して暗号化コンテンツデータE n c C Dを生成する(ステップS308)。暗号化部117は、生成した暗号化コンテンツデータE n c C Dをデータ記憶部213へ出力し、データ記憶部213は、暗号化コンテンツデータE n c C Dを受け取り(ステップS309)、データ記憶部213は、受け取った暗号化コンテンツデータE n c C Dを記憶する(ステップS310)。

6. 3 まとめ

15 以上説明したように、認証通信システム100bにおいて、コンテンツデータを暗号化するためのコンテンツ鍵を生成するのに、新たな乱数発生機構を必要とせず、アクセス情報の合成に用いる乱数発生機構と共有化できる。

7. その他の変形例

20 なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

25 (1) 上記の実施の形態において、デジタル著作物は、音楽の情報であるとしているが、小説や論文などの文字データ、コンピュータゲーム用のコンピュータプログラムソフトウェア、MP3などに代表される圧縮された音声データ、J P E Gなどの静止画像、M P E Gなどの動画像であるとしてもよい。

また、リーダライタ装置は、パーソナルコンピュータに限定されず、上記の様々なデジタル著作物を販売したり配布したりする出力装置であ

るとしてもよい。また、リーダライタ装置は、ヘッドホンステレオに限定されず、デジタル著作物を再生する再生装置であるとしてもよい。例えば、コンピュータゲーム装置、帯型情報端末、専用装置、パーソナルコンピュータなどであるとしてもよい。また、リーダライタ装置は、上記出力装置と再生装置との両方を兼ね備えているとしてもよい。

5 (2) 上記の実施の形態において、暗号アルゴリズム及び復号アルゴリズムは、DESを用いるとしているが、他の暗号を用いるとしてもよい。

また、上記実施の形態において、SHAを用いるとしているが、他の一方向性関数を用いるとしてもよい。

10 共通鍵、時変鍵の鍵長は、56ビットであるとしているが、他の長さの鍵を用いるとしてもよい。

(3) 上記の実施の形態において、合成部103は、アクセス情報と、乱数種の下位32ビットとを結合して、64ビット長の乱数化アクセス情報を生成しているが、これに限定されない。次のようにしてもよい。

15 合成部103は、32ビットのアクセス情報と、乱数種の下位32ビットとを1ビットずつ交互に結合して、64ビット長の乱数化アクセス情報を生成しているもよい。また、複数ビットずつ交互に結合してもよい。この場合、分離部206は、逆の操作を行うようとする。

20 (4) 上記の実施の形態において、メモリカード20の乱数生成部204は、乱数種記憶部202に記憶されている乱数種を用いて乱数R2を生成しているが、乱数生成部204は、乱数種を乱数R2として生成してもよい。

25 また、時変鍵生成部108、208は、R1及びR2を用いて時変鍵を生成しているが、応答値を用いるとしてもよい。また、共通鍵UKを絡ませてもよい。

(5) 認証通信システム100bにおいて、暗号化部117は、暗号化コンテンツデータEncCDをデータ記憶部213に書き込むとしてい

るが、暗号化コンテンツデータ E n c C D を機密データとして扱って、アクセス情報により示される領域に書き込むとしてもよい。

また、暗号化コンテンツ鍵 E n c C K を機密データとして扱わずに、データ記憶部 2 1 3 に書き込むとしてもよい。

5 また、暗号化部 1 1 4 及び暗号化部 1 1 7 のいずれか一方を無くし、残っている一方により共有化してもよい。

(6) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号である 10 としてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DV 15 D-RAM、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

20 また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(4) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとても

よい。

産業上の利用の可能性

デジタル著作物を出力する出力装置から半導体記録媒体へデジタル著作物を複製する場合において、出力装置と半導体記録媒体とが、相互に正当性を認証する場合に利用することができる。また、デジタル著作物の記録されている半導体記録媒体からデジタル著作物を読み出して再生する場合において、半導体記録媒体と再生装置との間で、各装置が、相互に正当性を認証する場合に利用することができる。

請 求 の 範 囲

1. デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、
5

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証フェーズと、

10 前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証フェーズと、

前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズと
15 を含むことを特徴とする認証通信システム。

2. 前記第1認証フェーズにおいて、

前記アクセス装置は、

20 前記領域を示すアクセス情報を取得するアクセス情報取得部と、

乱数を取得する乱数取得部と、

取得した前記アクセス情報と、取得した乱数とを合成して乱数化アクセス情報を生成する生成部と、

25 生成した乱数化アクセス情報を暗号アルゴリズムを施して攪乱化アクセス情報を生成する暗号部とを含み、

前記記録媒体は、

生成された攪乱化アクセス情報から応答値を生成する応答値生成部と
25 を含み、

前記アクセス装置は、
生成された前記応答値を用いて、前記記録媒体の正当性の認証を行う
認証部を含む

ことを特徴とする請求の範囲1に記載の認証通信システム。

5 3. 前記転送フェーズにおいて、

前記記録媒体は、

生成された攪乱化アクセス情報に復号アルゴリズムを施して乱数化ア
クセス情報を生成する復号部と、

伝送された乱数化アクセス情報からアクセス情報を分離する分離部と
10 を含む

ことを特徴とする請求の範囲2に記載の認証通信システム。

4. 前記第1認証フェーズにおいて、

前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を
含み、

15 前記乱数取得部は、乱数種記憶部から乱数種を読み出すことにより、
乱数を取得する

ことを特徴とする請求の範囲3に記載の認証通信システム。

5. 前記第1認証フェーズにおいて、

前記アクセス装置は、さらに、

20 前記攪乱化アクセス情報を乱数種として前記乱数種記憶部に上書きす
る

ことを特徴とする請求の範囲4に記載の認証通信システム。

6. 前記第1認証フェーズにおいて、

前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を
25 含み、

前記乱数取得部は、乱数種記憶部から乱数種を読み出し、読み出した
乱数種に基づいて乱数を生成することにより、乱数を取得する

ことを特徴とする請求の範囲3に記載の認証通信システム。

7. 前記第1認証フェーズにおいて、

前記アクセス装置は、さらに、

生成された前記乱数を乱数種として前記乱数種記憶部に上書きすることを特徴とする請求の範囲6に記載の認証通信システム。

5 8. 前記転送フェーズにおいて、

前記領域にデジタル情報を記録している記録媒体は、

前記アクセス情報により示される前記領域からデジタル情報を読み出し、読み出したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、

10 前記領域からデジタル情報を読み出す前記アクセス装置は、

生成された暗号化デジタル情報に復号アルゴリズムを施してデジタル情報を生成する復号部を含み、

前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号する

15 ことを特徴とする請求の範囲3に記載の認証通信システム。

9. 前記転送フェーズにおいて、

前記領域へデジタル情報を書き込む前記アクセス装置は、

デジタル情報を取得するデジタル情報取得部と、

取得したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、

20 前記記録媒体は、

生成された前記暗号化デジタル情報に復号アルゴリズムを施してデジタル情報を生成し、前記アクセス情報により示される前記領域へデジタル情報を書き込む復号部を含み、

25 前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号する

ことを特徴とする請求の範囲3に記載の認証通信システム。

10. 前記転送フェーズにおいて、

前記領域へデジタル情報を書き込む前記アクセス装置は、
デジタル情報を取得するデジタル情報取得部と、
コンテンツ鍵を取得するコンテンツ鍵取得部と、
取得したコンテンツ鍵に第1暗号アルゴリズムを施して暗号化コンテ
ンツ鍵を生成する第1暗号部と、
生成された前記暗号化コンテンツ鍵に第2暗号アルゴリズムを施して
二重暗号化コンテンツ鍵を生成する第2暗号化部と、
前記コンテンツ鍵を用いて、取得した前記デジタル情報に第2暗号ア
ルゴリズムを施して暗号化デジタル情報を生成する第3暗号部とを含み、
前記記録媒体は、
生成された前記二重暗号化コンテンツ鍵に第1復号アルゴリズムを施
して暗号化コンテンツ鍵を生成し、前記アクセス情報により示される前
記領域へ暗号化コンテンツ鍵を書き込む復号部を含み、
前記記録媒体は、さらに、生成された前記暗号化デジタル情報を記憶
する領域を含む
ことを特徴とする請求の範囲3に記載の認証通信システム。
11. デジタル情報を記憶する領域を有する記録媒体と、前記領域からデ
ジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス
装置とから構成される認証通信システムで用いられる認証通信方法であ
って、
前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報
を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記ア
クセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録
媒体の正当性の認証を行う第1認証ステップと、
前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証ステ
ップと、
前記記録媒体と前記アクセス装置とがともに正当性を有すると認証さ
れた場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアク

セス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップとを含むことを特徴とする認証通信方法。

5 12. デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記記録媒体と前記アクセス装置との間において各機器の正当性の認証を行った後に、デジタル情報を転送する認証通信システムで用いられる認証通信プログラムを記録しているコンピュータ
10 読み取り可能な記録媒体であって、

前記認証通信プログラムは、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証ステップと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証ステップと、

前記記録媒体と前記アクセス装置とともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップとを含むことを特徴とする記録媒体。

25 13. 請求の範囲1に記載の認証通信システムを構成するアクセス装置。

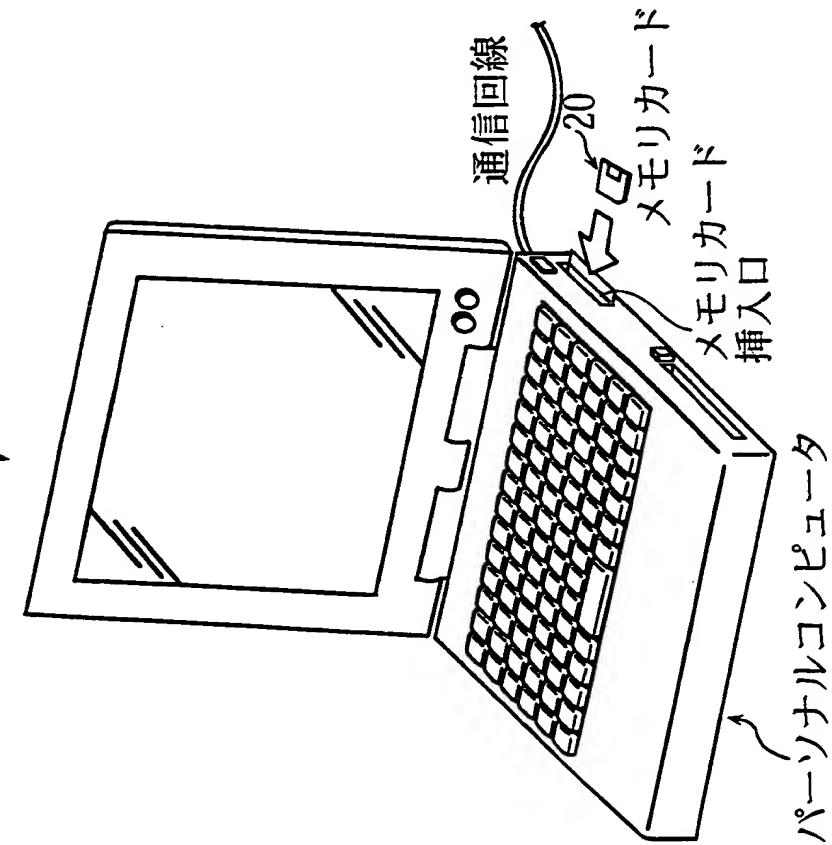
14. 請求の範囲2に記載の認証通信システムを構成するアクセス装置。

15. 請求の範囲 1 に記載の認証通信システムを構成する記録媒体。

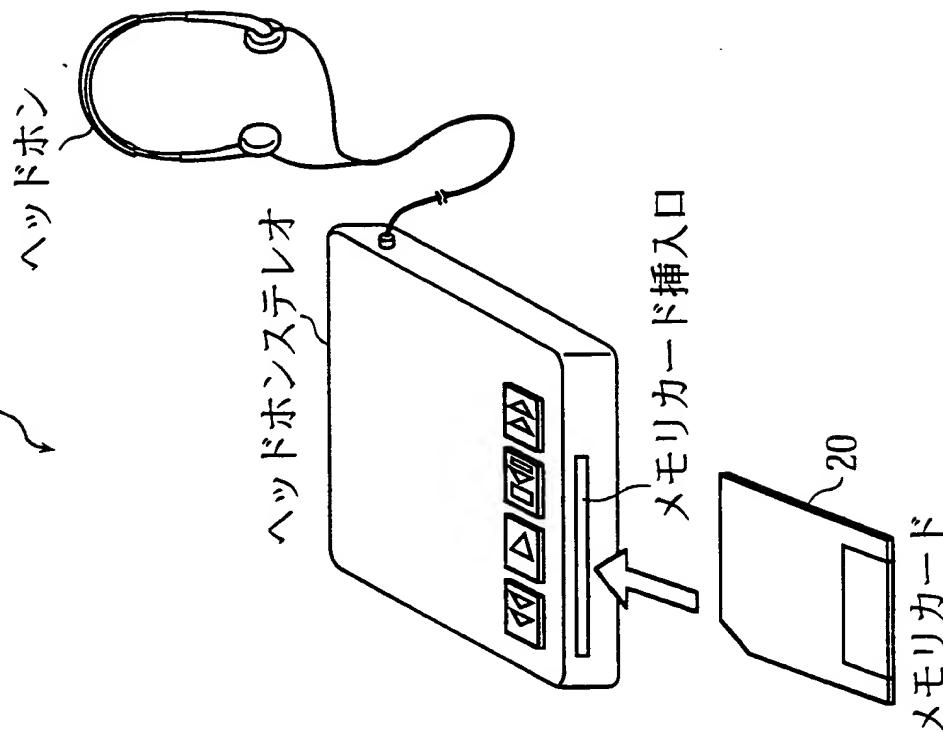
16. 請求の範囲 3 に記載の認証通信システムを構成する記録媒体。

図二

(a) 30 認証通信システム

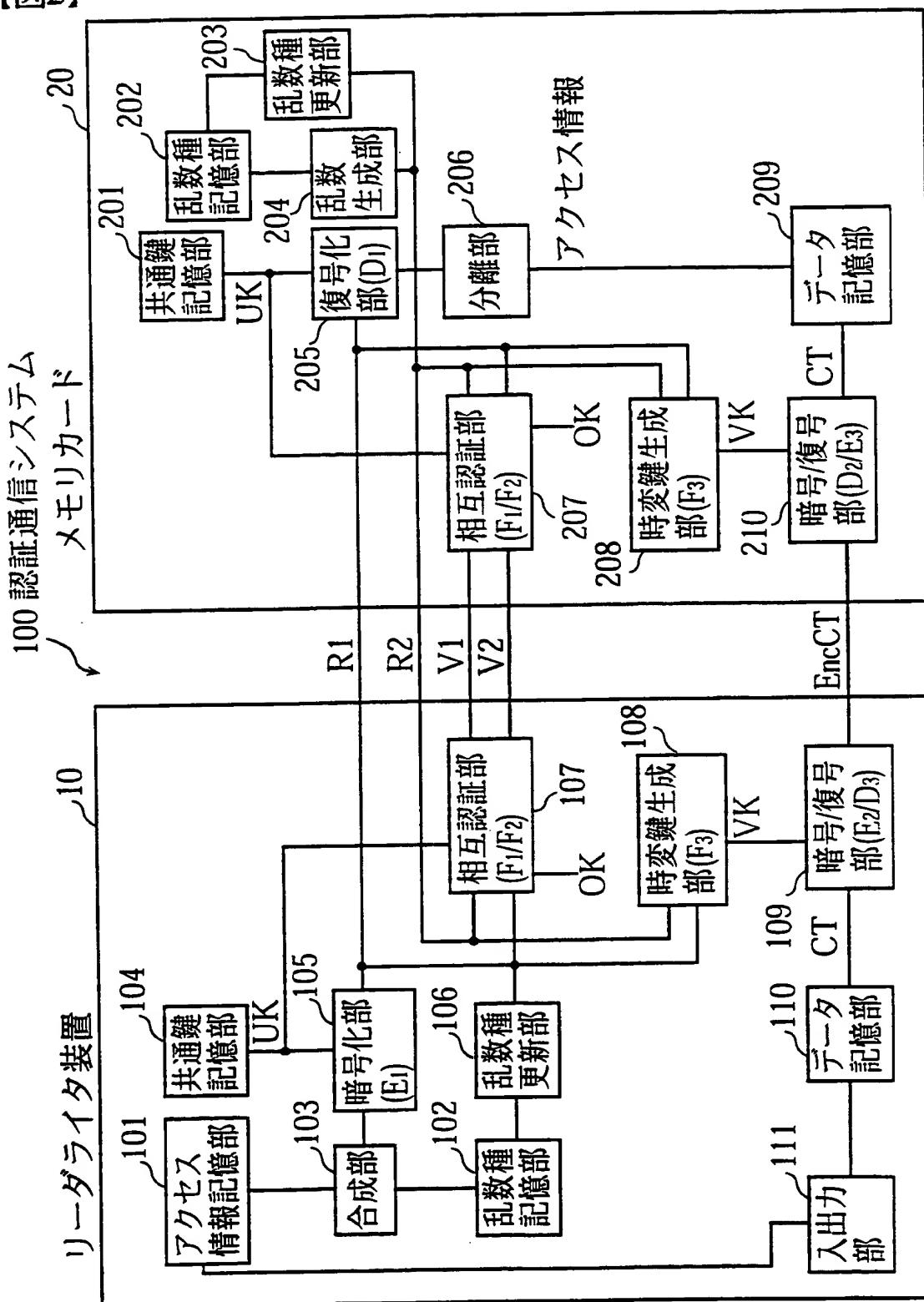


(b) 31 認証通信システム



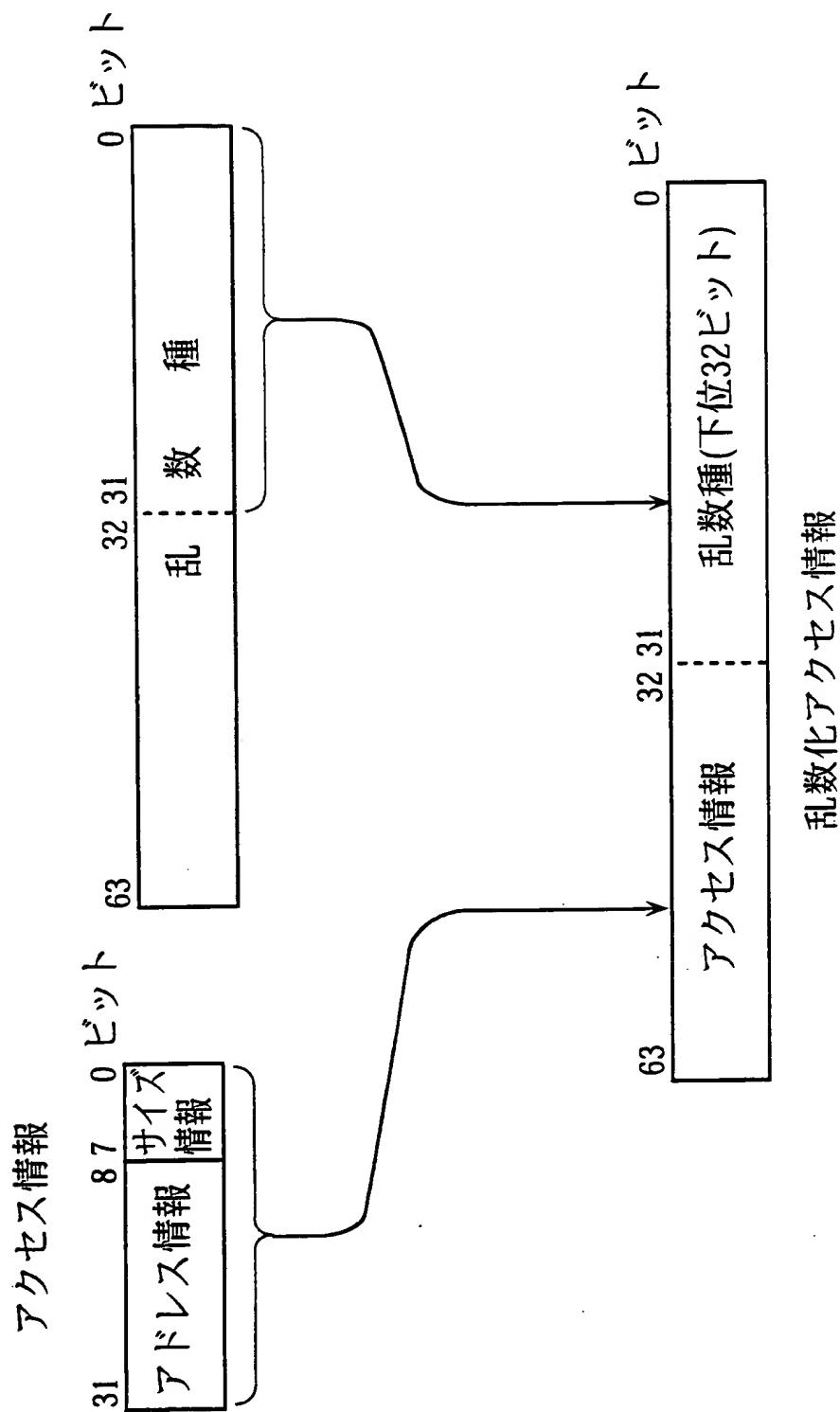
THIS PAGE BLANK (USPTO)

【図2】



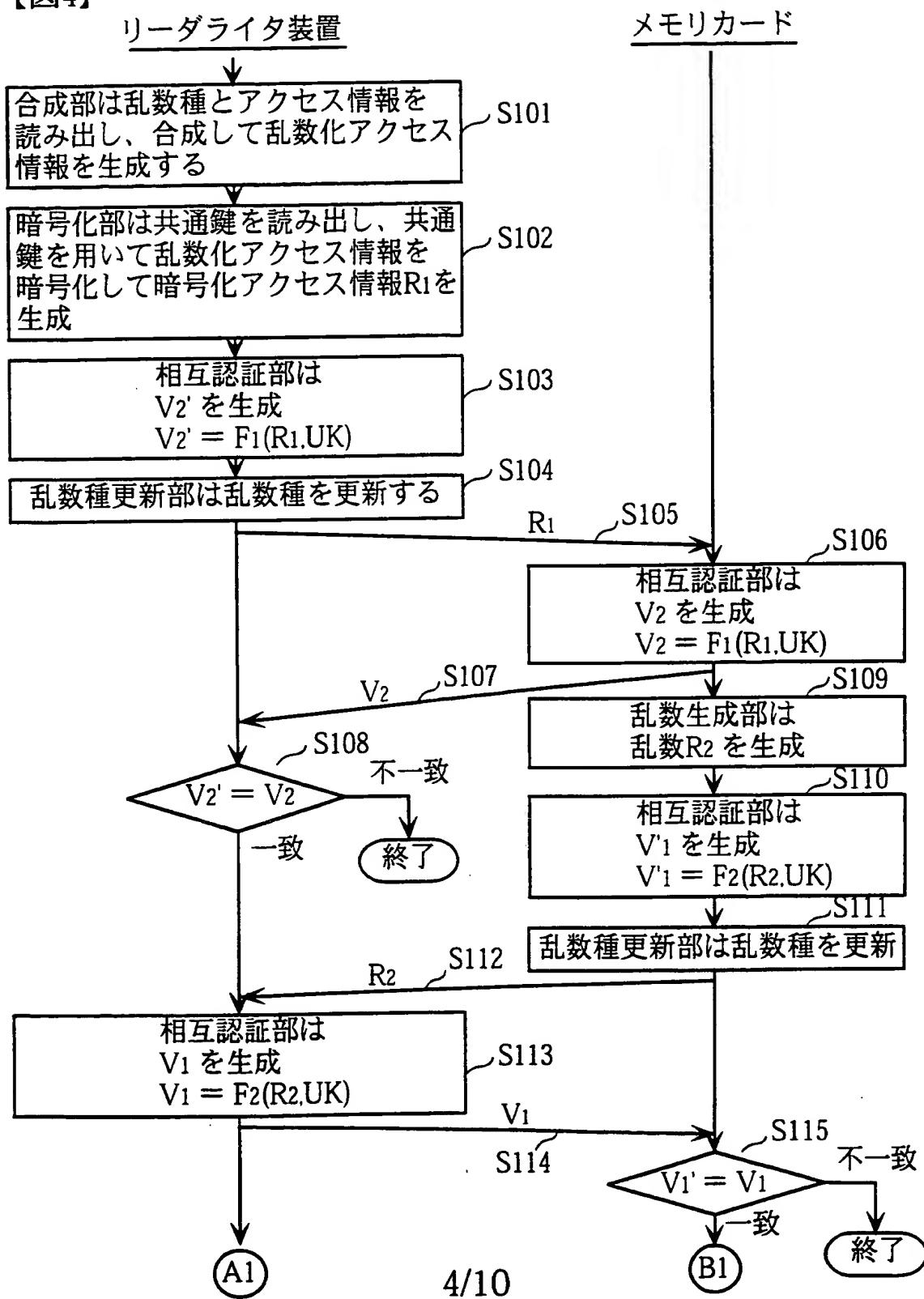
THIS PAGE BLANK (USPTO)

【図3】



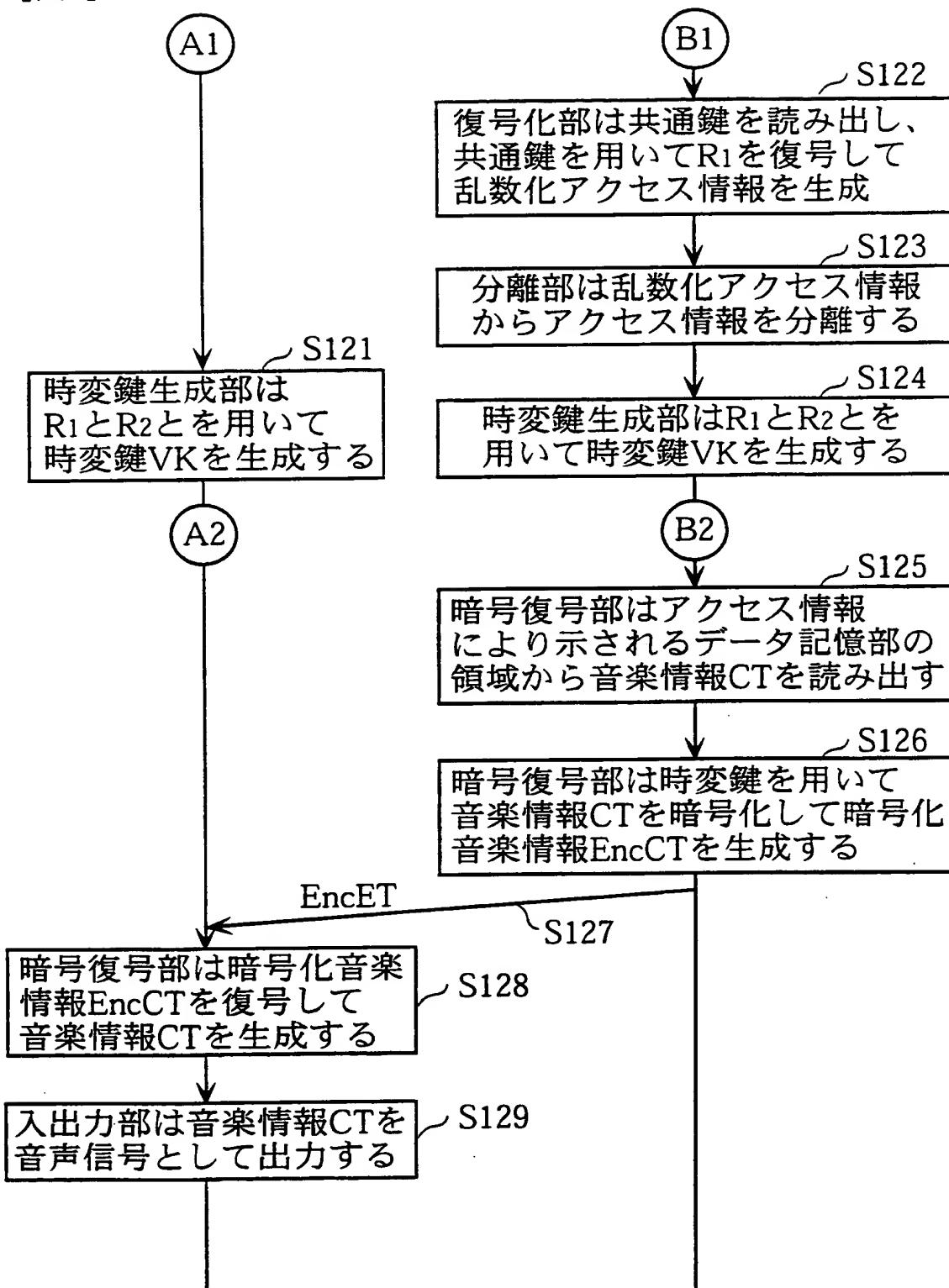
THIS PAGE BLANK (USPTO)

【図4】



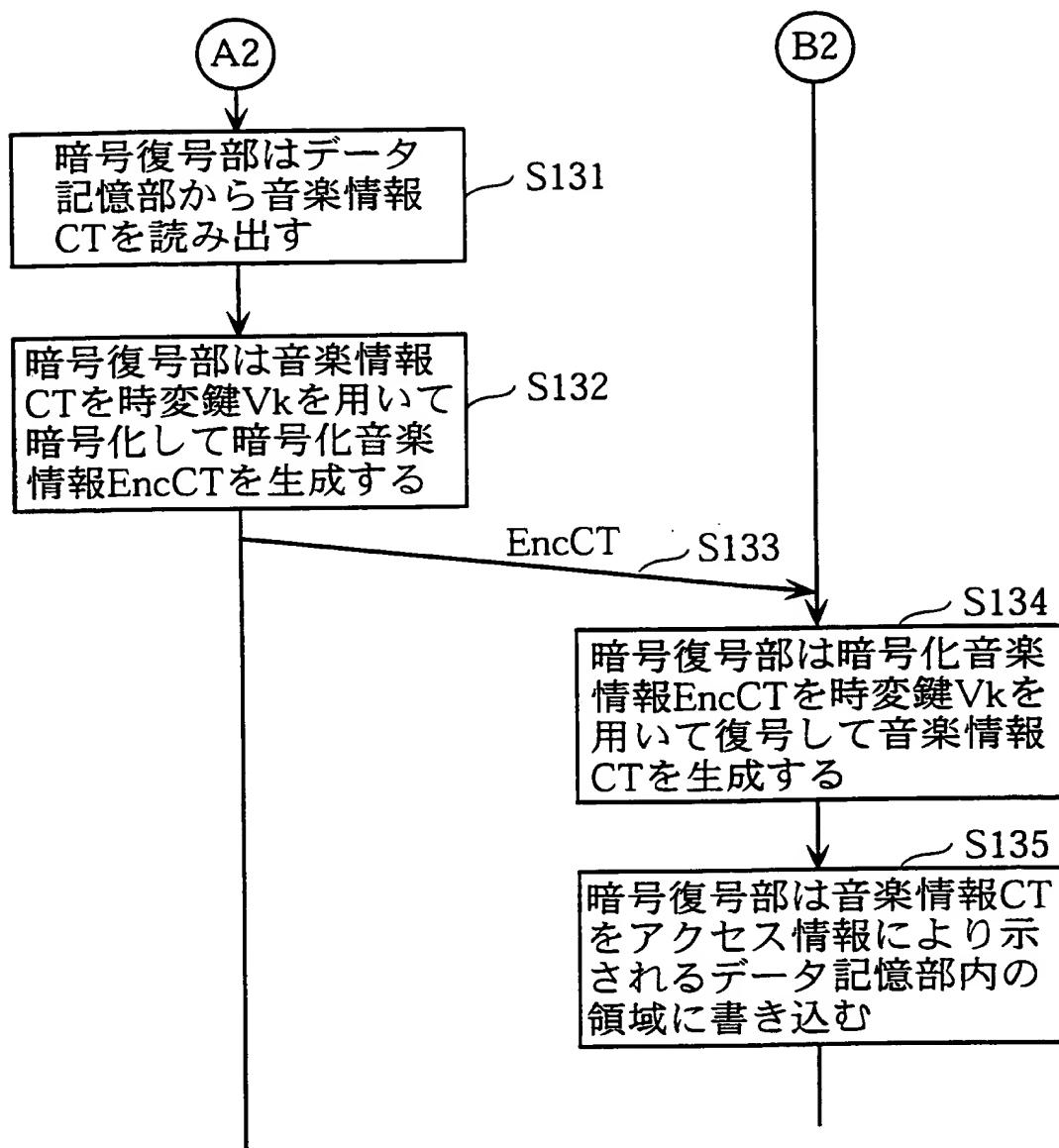
THIS PAGE BLANK (USPTO)

【図5】



THIS PAGE BLANK (USPTO)

【図6】



THIS PAGE BLANK (USPTO)

[図7]

100a 認証通信システム
メモリカード

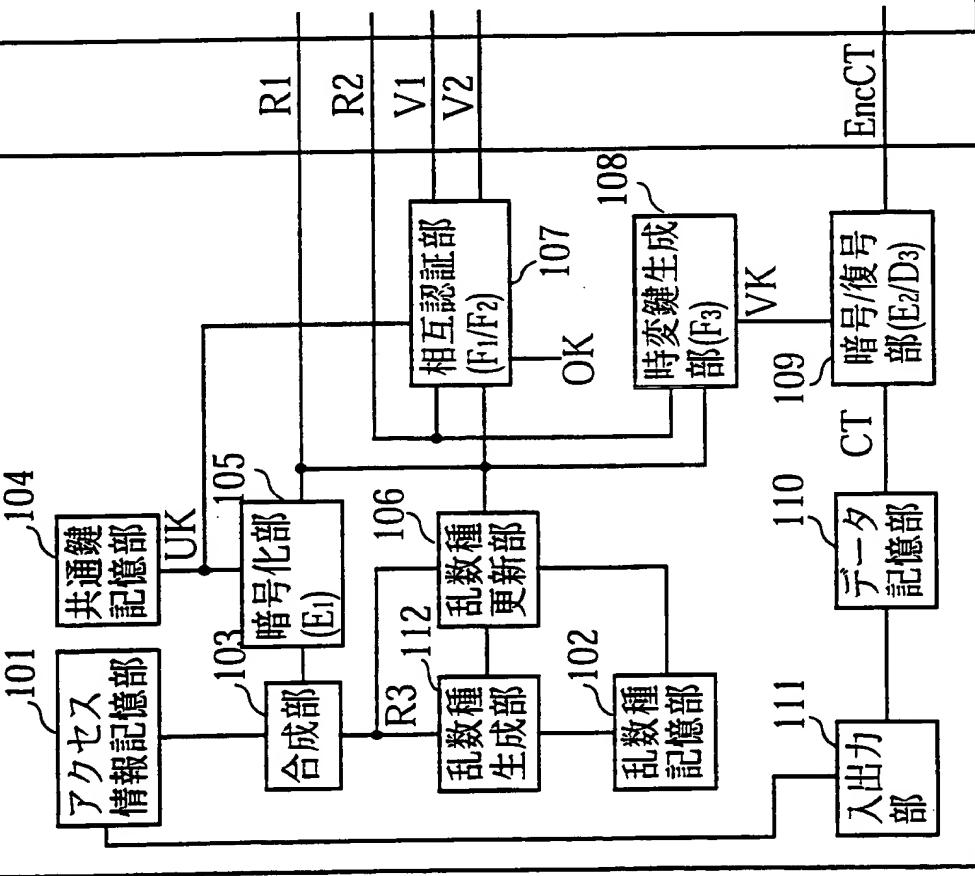
20

10a

リーダライタ装置

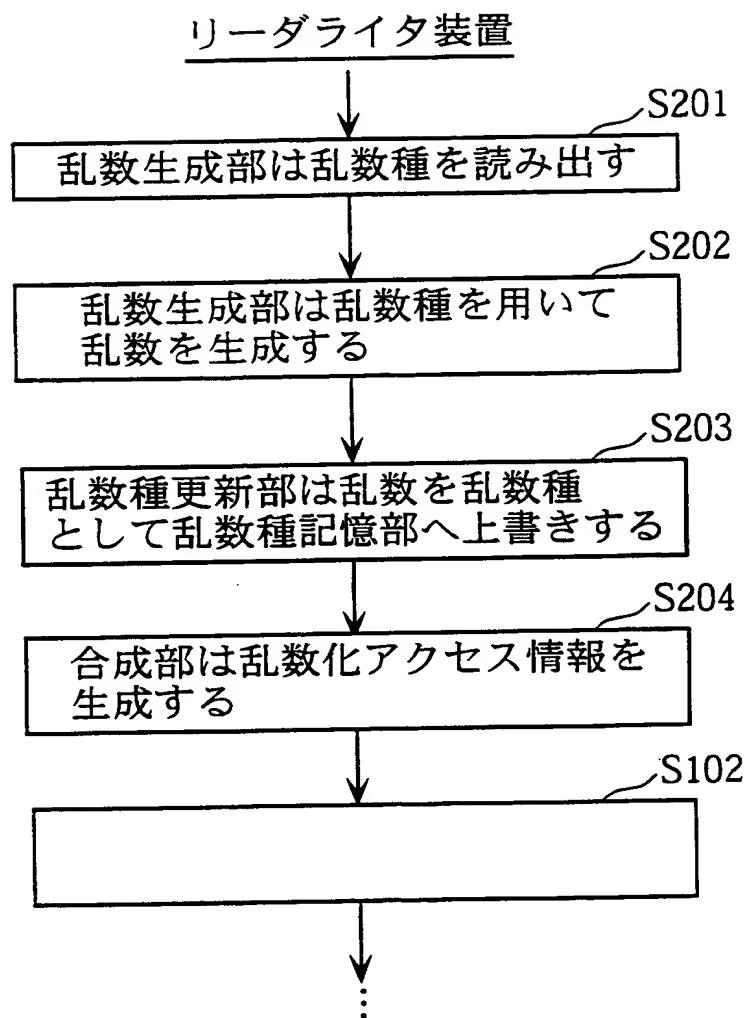
104

101



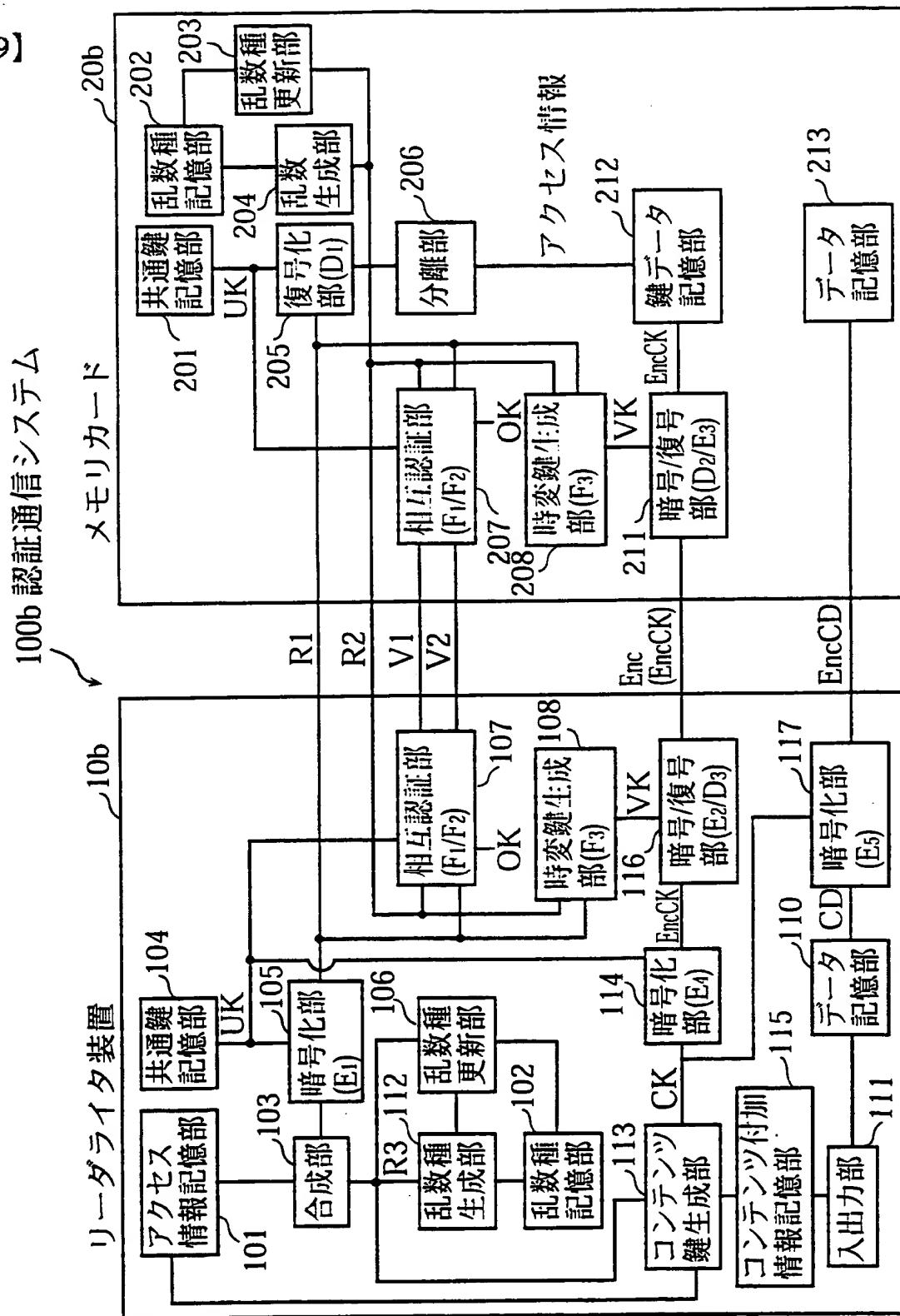
THIS PAGE BLANK (USPTO)

【図8】

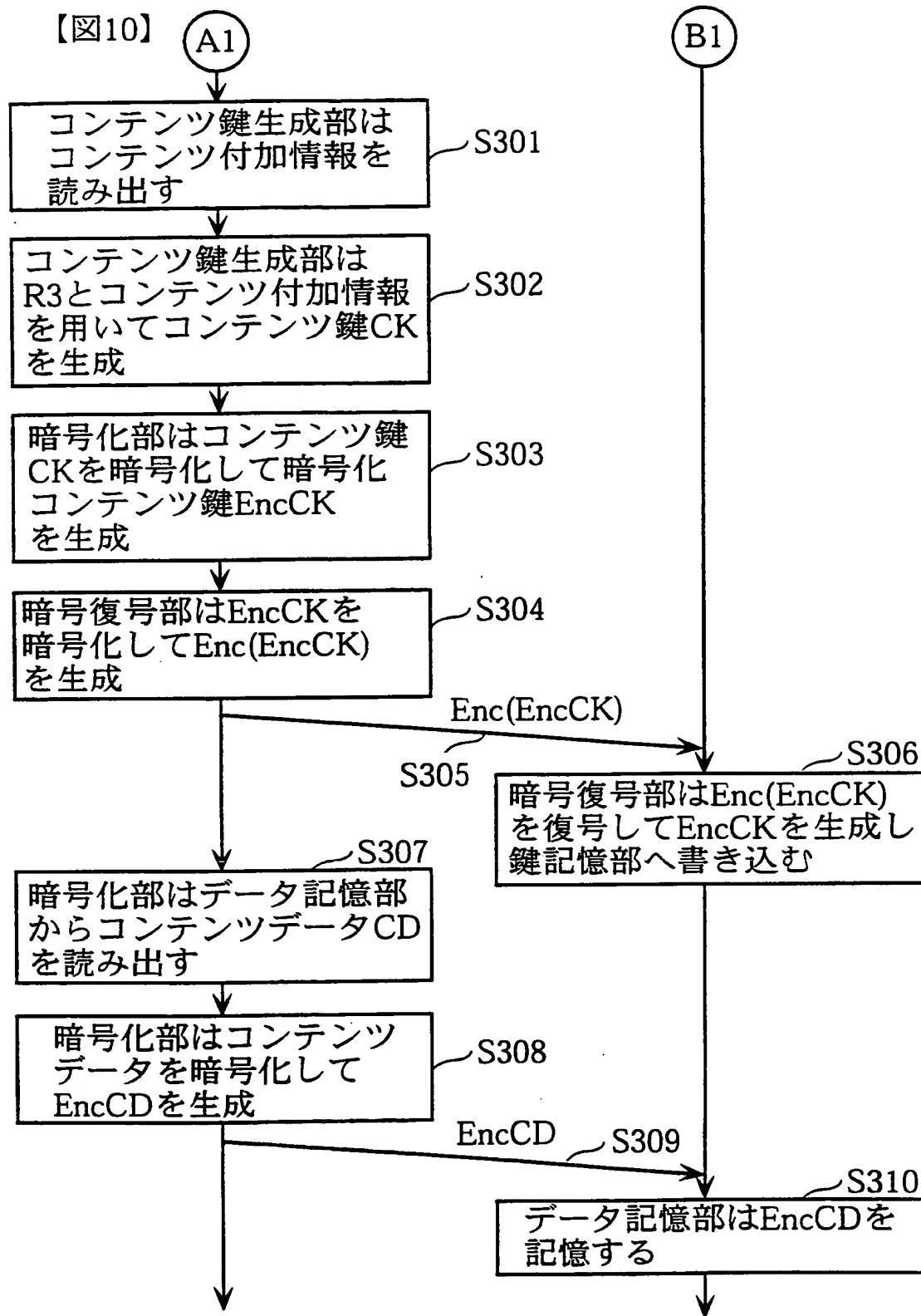


THIS PAGE BLANK (USPTO)

[圖9]



THIS PAGE BLANK (USPTO)



THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00159

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L9/32, H04L9/08, G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L9/32, H04L9/08, G06F17/60Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-51439, A (Matsushita Electric Ind. Co., Ltd.), 20 February, 1998 (20.02.98), Full text; Figs. 1 to 12 & EP, 809379, A & CN, 1170995, A & US, 6058476, A	1-16
Y	JP, 11-306673, A (Toshiba Corporation), 05 November, 1999 (05.11.99), Par. Nos. [0022] to [0024]; [0045]- [0052]; Figs. 1 to 15 (Family: none)	1-16
Y	JP, 8-56387, A (ALPINE ELECTRONICS, INC.), 27 February, 1996 (27.02.96), Par. Nos. [0007] to [0009]; Figs. 2 to 4 (Family: none)	2-6
Y	JP, 7-311674, A (Nippon Telegr. & Teleph. Corp. <NTT>), 28 November, 1995 (28.11.95), Par. Nos. [0019], [0027] to [0028]; Par. No. [0040]; Figs. 1 to 3 (Family: none)	4-7
A	JP, 11-265317, A (Nippon Telegr. & Teleph. Corp. <NTT>), 28 September, 1999 (28.09.99),	1-16

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means		
"P" document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
05 April, 2001 (05.04.01)Date of mailing of the international search report
17 April, 2001 (17.04.01)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/00159

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>Full text; Figs. 1 to 10 (Family: none)</p> <p>Nobuyoshi YAMAMOTO et al., "Multimedia on Demand Service ni okeru Joho Hogo System," NTT R & D, Vol.44, No.10 (10.09.95) pp.813-818</p>	1-16

国際調査報告

国際出願番号 PCT/JP01/00159

A. 発明の属する分野の分類(国際特許分類(IPC))

Int. Cl' H04L9/32, H04L9/08, G06F17/60

B. 調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

Int. Cl' H04L9/32, H04L9/08, G06F17/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926-1996年
日本国公開実用新案公報	1971-2001年
日本国登録実用新案公報	1994-2001年
日本国実用新案登録公報	1996-2001年

国際調査で使用した電子データベース(データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 10-51439, A (松下電器産業株式会社) 20. 2月. 1998 (20. 02. 98) 全文, 図1-12 & EP, 809379, A & CN, 1170995, A & US, 6058476, A	1-16
Y	JP, 11-306673, A (株式会社東芝) 5. 11月. 1999 (05. 11. 99) 第【0022】-【0024】段落, 第【0045】- 【0052】段落, 図1-15 (ファミリーなし)	1-16

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- 「A」特に関連のある文献ではなく、一般的技術水準を示すもの
- 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
- 「I」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す)
- 「O」口頭による開示、使用、展示等に言及する文献
- 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
- 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
- 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
- 「&」同一パテントファミリー文献

国際調査を完了した日

05. 04. 01

国際調査報告の発送日

17.04.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官(権限のある職員)

青木 重徳

印

5M 4229

電話番号 03-3581-1101 内線 3597

C(続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 8-56387, A (アルパイン株式会社) 27. 2月. 1996 (27. 02. 96) 第【0007】-【0009】段落, 図2-4 (ファミリーなし)	2-6
Y	JP, 7-311674, A (日本電信電話株式会社) 28. 11月. 1995 (28. 11. 95) 第【0019】段落, 第【0027】-【0028】段落, 第【0040】段落, 図1-3 (ファミリーなし)	4-7
A	JP, 11-265317, A (日本電信電話株式会社) 28. 9月. 1999 (28. 09. 99) 全文, 図1-10 (ファミリーなし)	1-16
A	山本喜義 他: “マルチメディアオンデマンドサービスにおける情報保護システム” NTT R&D, Vol. 44, No. 10 (10. 09. 95) pp. 813-818	1-16